REMARKS/ARGUMENTS

In the Office Action, the Examiner noted that claims 1-15 and 17-26 are pending in the application. The Examiner additionally stated that claims 1-15 and 17-26 are rejected. By this communication, claims 7, 21, and 26 are cancelled and claims 1, 8, 17, and 22 are amended. Hence, claims 1-6, 8-15, 17-20, and 22-25 are pending in the application.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

In the Specification

The Examiner objected to the disclosure because it contains an embedded hyperlink and/or other form of browser-executable code, and it was required of the Applicant to delete the hyperlink and/or other form of browser-executable code.

By this communication, the objected to matter is cancelled and it is therefore requested that the objection to the disclosure be withdrawn.

In addition, Applicant has amended the specification to secure a substantial correspondence between the claims amended herein and the remainder of the specification. No new matter is presented.

In the Claims

Rejections Under 35 U.S.C. §112

The Examiner rejected claims 1, 17, and 22 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement, noting that the claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The Examiner stated that Applicant has amended the claim 1, 17 and 22 and paragraphs [0020.1], [0021] and [0022] in the specification to include the following limitation: "The instruction register is within the microprocessor and has a cryptographic instruction disposed therein. The cryptographic instruction is part of an application program, and the microprocessor

executes the application program." The Examiner remarked that it is unclear where applicant has support for the above limitations.

Applicant respectfully traverses the Examiner's rejections and notes that the discussion with reference to FIGURE 3 provides support for the noted amendments. More specifically, paragraphs [0044] through [0046] discuss the instruction register 302 within the microprocessor 301 having the cryptographic instruction XCRYPT disposed therein. The first and second sentences in paragraph [0046] provides support for the amendment, "the cryptographic instruction is part of an application program, and the microprocessor executes the application program."

Accordingly, it is requested that the rejections be withdrawn.

Rejections Under 35 U.S.C. §103(a)

The Examiner rejected claims 1-6, 8-15, 17-20, and 22-25 under 35 U.S.C. 103(a) as being unpatentable over Kessler et al. (US 6789147), hereinafter, "Kessler," in view of Harrison et al. (US 6,101,255), hereinafter, "Harrison." Applicant respectfully traverses the Examiner's rejections.

As per claims 1, 17, and 22, the Examiner noted that Kessler discloses an apparatus for performing cryptographic operations, comprising:

- an instruction register within a microprocessor (Fig. 1, item 10) having a cryptographic instruction disposed therein (column 3, lines 40-45), wherein said cryptographic instruction is part of an application program, and wherein said microprocessor executes said application program, and wherein said cryptographic instruction prescribes one of the cryptographic operations, and wherein said cryptographic instruction prescribes that a user-generated key schedule be employed for execution of said one of the cryptographic operations (noting that the execution units include a plurality of operation blocks that correspond to different cryptographic operations that are used depending upon the type of instruction received in the execution queue, and that the operation blocks correspond to cryptographic algorithms such as AES, 3DES, DES, and RC4) (column 9, lines 8-42; Fig. 8);

- a keygen unit, operatively coupled to said instruction register, configured to direct said microprocessor to load said user-generated key schedule (column 12, lines 7-40); and
- an execution unit, operatively coupled to said keygen unit, configured to employ said user-generated key schedule to execute said one of the cryptographic operations (column 9, lines 7-43), said execution unit comprising:
    - a cryptography unit, configured execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by a control word that is provided to said cryptography unit (noting that the primitive security operation blocks include an Advanced Encryption Standard (AES) block 807, a Triple Data Encryption Standard (3DES) block 809, a modular exponentiation block 811, a hash block 813, a simple arithmetic and logic block 815, and an alleged RC4.RTM. block 819) (column 9, lines 8-22).

The Examiner conceded that Kessler el al. do not explicitly specify wherein said cryptographic instruction is part of an application program, and wherein said microprocessor executes said application program, but that Harrison et al. disclose a programmable cryptographic processing system and method, which further disclose wherein said cryptographic instruction is part of an application program, and wherein said microprocessor executes said application program(column 2, lines 34-57; column 5, lines 48-55; column 8, lines 37-53; Fig. 5).

The Examiner thus concluded that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Kessler et al such as to use the co-processor of Kessler et al. to execute the actual application program as described by Harrison et al. in order to rapidly and securely switches programs and context on each data unit processed as taught by Harrison et al (column 1, lines 38-62).

Applicant has considered the Examiner's points in the new grounds for rejection and has thus amended claims 1, 17, and 22 to recite, substantially, that the microprocessor is an

x86-compatible microprocessor and that the cryptographic instruction is arranged according to the instruction format for execution on the x86-compatible microprocessor. Thus, the instant amendments are provided to clearly distinguish the present invention over the interface taught by Kessler and the programmable crypto processing system taught by Harrison.

Applicant submits that a single x86-formated cryptographic instruction as part of an application program which is executed by an x86-compatible microprocessor according to the present invention is not contemplated by either one of the cited references, alone or in combination. A specific disclosure of an x86-compatible microprocessor is provided in the instant specification in numerous paragraphs, with the following example from paragraph [0044] provided below for ease of reference:

> "In one embodiment that is compatible with the x86 architecture, the cryptography unit 316 operates in parallel with an x86 integer unit, an x86 floating point unit, an x86 MMX® unit, and an x86 SSE® unit. According to the scope of the present application, an embodiment is compatible with the x86 architecture if the embodiment can correctly execute a majority of the application programs that are designed to be executed on an x86 microprocessor. An application program is correctly executed if its expected results are obtained."

Support for formatting of the cryptographic instruction according to the x86 instruction format is provided in, *inter alia,* paragraphs [0044], [0045], and [0046].

Never is it contemplated, or even suggested, that a x86-compatible microprocessor capable of executing an application program be employed to execute a cryptographic instruction as part of the application program to perform a specified cryptographic operation because, at the time of invention, there was no existing mechanism that allowed for the execution of cryptographic operations by a general-purpose x86-compatible microprocessor other than via executing a complex and long series of instructions, typically obtained through an operating system call. In addition, it is further submitted that the teachings of Harrison and Kessler in combination teach away from a host x86-

compatible microprocessor based approach for performing cryptographic operations, for the suggestion of a cryptographic coprocessor system (Harrison) for performing cryptographic operations combined with a coprocessor interface (Kessler) leads one toward a cryptographic coprocessor implementation.

In contrast to the combined teachings of Harrison and Kessler, Applicant realized that provision of an atomic cryptographic instruction for use in an application program and inclusion of a cryptographic unit within the execution logic of a x86-compatible microprocessor whereby the cryptographic instruction could be executed as part of the operations performed when the x86-compatible microprocessor executes the application program would overcome the disadvantages associated with the approach resulting from a combination of the teachings of Harrison and Kessler. It is thus a feature of the present invention to allow for use of the cryptographic instruction at the application level (i.e., within an application program as opposed to an operating system call), thus overcoming the disadvantages of present day coprocessor implementations.

Accordingly, it is requested that the rejections of claims 1, 17, and 22 be withdrawn.

With respect to claims 2-6 and 8-15, these claims depend from claim 1 and add further limitations that are neither anticipated nor made obvious by Harrison, Kessler, or a combination of Harrison and Kessler. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 2-6 and 8-15.

With respect to claims 18-20, these claims depend from claim 17 and add further limitations that are neither anticipated nor made obvious by Harrison, Kessler, or a combination of Harrison and Kessler. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 18-20.

Claims 23-25 depend from claim 22 and add further limitations that are neither anticipated nor made obvious by Harrison, Kessler, or a combination of Harrison and Kessler. Accordingly, Applicant respectfully submits that claims 23-25 are allowable as well.

The Examiner also rejected claims 7, 21, and 26 under 35 U.S.C. 103(a) as being unpatentable over Kessler, in view of Harrison, and further in view of Miller (US 6081884), hereinafter, "Miller."

By this amendment, claims 7, 21, and 26 are cancelled thereby rendering the rejections moot.

CONCLUSIONS

Applicant believes this to be a complete response to all of the issues raised in the instant office action and further submits, in view of the amendments and arguments advanced above, that claims 1-6, 8-15, 17-20, and 22-25 are in condition for allowance. Reconsideration of the rejections is requested, and allowance of the claims is solicited.

Applicant also notes that any amendments made by way of this response, and the observations contained herein, are made solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent business Goals (PBG), 65 Fed. Reg. 54603 (September 8, 2000), and are furthermore made without prejudice to Applicant under this or any other jurisdictions. It is moreover asserted that insofar as any subject matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments made herein and/or incorporated in attachments submitted with this response, Applicants wishes to reserve the right and hereby provides notice of intent to restore such subject matter and/or file a continuation application in respect thereof.

Applicant earnestly requests that the Examiner contact the undersigned practitioner by telephone if the Examiner has any questions or suggestions concerning this amendment, the application, or allowance of any claims thereof.

Respectfully submitted,
HUFFMAN PATENT GROUP, LLC

/Richard K. Huffman/

By: _____

RICHARD K. HUFFMAN, P.E.
Registration No. 41,082
Tel: (719) 575-9998

12/28/2008

Date: _____